# AN ASYMPTOTIC FORMULA FOR THE NUMBER OF IRREDUCIBLE TRANSFORMATION SHIFT REGISTERS

STEPHEN D. COHEN, SARTAJ UL HASAN, DANIEL PANARIO, AND QIANG WANG

Abstract. We consider the problem of enumerating the number of irreducible transformation shift registers. We give an asymptotic formula for the number of irreducible transformation shift registers in some special cases. Moreover, we derive a short proof for the exact number of irreducible transformation shift registers of order two using a recent generalization of a theorem of Carlitz.

## 1. Introduction

Linear feedback shift registers (LFSRs) are devices that are used to generate sequences over a finite field. This sort of sequence has received numerous applications in various disciplines including in the design of stream ciphers; see, for example, [12, 15]. For all practical purposes, these sequences are generally considered over a binary field. The sequences with maximal period have been proved to have good cryptographic properties. LFSRs corresponding to sequences with maximum period are known as primitive LFSRs.

The number of primitive LFSRs of order $n$ over a finite field $\mathbb{F}_q$ is given by

$$\frac{\phi(q^n-1)}{n}, \tag{1}$$

where $\phi$ is Euler's totient function. A similar formula for the number of irreducible LFSRs (that is, when the characteristic polynomial of the LFSR is irreducible) of order $n$ over a finite field $\mathbb{F}_q$ is given by

$$\frac{1}{n}\sum_{d|n}\mu\left(d\right)q^{\frac{n}{d}}, \tag{2}$$

where $\mu$ is the Möbius function.

Niederreiter [16] introduces the notion of *multiple recursive matrix method*, which may be considered as a generalization of the classical LFSRs. Zeng et. al [21] consider the notion of $\sigma$-LFSR which is a word-oriented stream cipher. It turns out that the latter is essentially same as Niederreiter's multiple recursive matrix method. A conjectural formula for the number of primitive $\sigma$-LFSRs of order $n$ was given in the binary case in [21]. An extension of this conjectural formula over the finite field $\mathbb{F}_{q^m}$ given in [10] states that this number is

$$\frac{\phi(q^{mn}-1)}{mn}q^{m(m-1)(n-1)}\prod_{i=1}^{m-1}(q^m-q^i). \tag{3}$$

*Date*: June 9, 2015.

2010 *Mathematics Subject Classification.* 15B33, 12E20, 11T71 and 12E05.

*Key words and phrases.* Block companion matrix; characteristic polynomial; irreducible polynomial; primitive polynomial; Galois group; transformation shift register.

We refer to [10] and [11] for recent progress on this conjecture and to [4] for a proof of this conjecture.

It is also known from [11] and [4], see also [18], that the number of irreducible $\sigma$-LFSRs is

$$\frac{1}{mn} q^{m(m-1)(n-1)} \prod_{i=1}^{m-1} (q^m - q^i) \sum_{d|mn} \mu(d)\, q^{\frac{mn}{d}}. \tag{4}$$

We focus on *transformation shift registers* (TSRs) in this paper. This notion was introduced by Tsaban and Vishne [20] and it can be also considered as a generalization of classical LFSRs. The notion of TSR was introduced to address a problem of Preneel [17] on designing fast and secure LFSRs with the help of the word operations of modern processors and the techniques of parallelism. It may be noted that the family of TSRs is a subclass of the family of $\sigma$-LFSRs. Dewar and Panario [8, 9] further studied the theory of TSRs.

We do not know yet any explicit formula like (1) and (3) for the number of primitive TSRs. The problem of enumerating primitive TSRs was first considered in [13]. It was proved that in order to count primitive TSRs, it is sufficient to enumerate certain block companion matrices in a corresponding general linear group. However, except few initial cases, this problem seems rather difficult and still remains open.

Based on some empirical evidence, Tsaban and Vishne [20] pointed out that irreducible TSRs contain a high proportion of primitive TSRs. Thus in order to find a primitive TSR in practice one might try an exhaustive search only among the irreducible ones instead of over all TSRs; there is a high chance that one might end up getting a primitive TSR in this way. This reduces the search complexity of primitive TSRs. Motivated by this fact and in an attempt to obtain a nice formula like (2) and (4), we consider here the problem of enumerating irreducible TSRs. In fact, this problem was first considered in [18] where the author gives a formula for the number of irreducible TSRs of order two. Moreover, in [18], as a consequence of this result, a new proof of a theorem of Carlitz about the number of the self reciprocal irreducible monic polynomials of a given degree over a finite field is deduced.

Our paper is organized in the following manner. In Section 2 we recall some results concerning transformation shift registers needed in this work.

As it has been mentioned earlier, Ram [18] gives a formula for the number of irreducible TSRs of order two. In Section 3 we give a short proof of Ram's result using a variant of a theorem of Carlitz recently proved [1]. Asymptotic analysis of the number of irreducible TSRs of order two is carried out in Section 4. Finally, in Section 5, we prove an asymptotic formula for the number of irreducible TSRs of any order when $q$ is odd.

## 2. Transformation Shift Registers

We denote by $\mathbb{F}_q$ the finite field with $q = p^r$ elements, where $p$ is a prime number and $r$ is a positive integer, and by $\mathbb{F}_q[X]$ the ring of polynomials in one variable $X$ with coefficients in $\mathbb{F}_q$. For every set $S$, we denote by $|S|$, the cardinality of the set $S$. Also we denote by $M_d(\mathbb{F}_q)$, the set of all $d \times d$ matrices with entries in $\mathbb{F}_q$. We now recall from [13] some definitions and results concerning transformation shift registers.

Throughout this and subsequent sections, we fix positive integers $m$ and $n$, and a vector space basis $\{\alpha_0, \dots, \alpha_{m-1}\}$ of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$. Given any $s \in \mathbb{F}_{q^m}$, there are unique $s_0, \dots, s_{m-1} \in \mathbb{F}_q$ such that $s = s_0\alpha_0 + \cdots + s_{m-1}\alpha_{m-1}$, and we shall denote the corresponding co-ordinate vector $(s_0, \dots, s_{m-1})$ of $s$ by $\mathbf{s}$. Evidently, the association $s \longmapsto \mathbf{s}$ gives a vector space isomorphism of $\mathbb{F}_{q^m}$ onto $\mathbb{F}_q^m$. Elements of $\mathbb{F}_q^m$ may be thought of as row vectors and so $\mathbf{s}C$ is a well-defined element of $\mathbb{F}_q^m$ for any $\mathbf{s} \in \mathbb{F}_q^m$ and $C \in M_m(\mathbb{F}_q)$.

**Definition 2.1.** Let $c_0, c_1, \dots, c_{n-1} \in \mathbb{F}_q$ and $A \in M_m(\mathbb{F}_q)$. Given any $n$-tuple $(\mathbf{s}_0, \dots, \mathbf{s}_{n-1})$ of elements of $\mathbb{F}_{q^m}$, let $(\mathbf{s}_i)_{i=0}^{\infty}$ denote the infinite sequence of elements of $\mathbb{F}_{q^m}$ determined by the following linear recurrence relation:

$$\mathbf{s}_{i+n} = \mathbf{s}_i(c_0A) + \mathbf{s}_{i+1}(c_1A) + \cdots + \mathbf{s}_{i+n-1}(c_{n-1}A) \quad i = 0, 1, \dots. \tag{5}$$

The system (5) is a *transformation shift register* (TSR) of order $n$ over $\mathbb{F}_{q^m}$, while the sequence $(\mathbf{s}_i)_{i=0}^{\infty}$ is the *sequence generated by the TSR* (5). The $n$-tuple $(\mathbf{s}_0, \mathbf{s}_1, \dots, \mathbf{s}_{n-1})$ is the *initial state* of the TSR (5) and the polynomial $I_mX^n - (c_{n-1}A)X^{n-1} - \cdots - (c_1A)X - (c_0A)$ with matrix coefficients is the *tsr-polynomial* of the TSR (5), where $I_m$ denotes the $m \times m$ identity matrix over $\mathbb{F}_q$. The sequence $(\mathbf{s}_i)_{i=0}^{\infty}$ is *ultimately periodic* if there are integers $r, n_0$ with $r \geq 1$ and $n_0 \geq 0$ such that $\mathbf{s}_{j+r} = \mathbf{s}_j$ for all $j \geq n_0$. The least positive integer $r$ with this property is the *period* of $(\mathbf{s}_i)_{i=0}^{\infty}$ and the corresponding least nonnegative integer $n_0$ is the *preperiod* of $(\mathbf{s}_i)_{i=0}^{\infty}$. The sequence $(\mathbf{s}_i)_{i=0}^{\infty}$ is *periodic* if its preperiod is 0.

The following proposition gives some basic facts about TSRs.

**Proposition 2.2.** [13] *For the sequence $(\mathbf{s}_i)_{i=0}^{\infty}$ generated by the TSR* (5) *of order $n$ over $\mathbb{F}_{q^m}$, we have*

- (i) *$(\mathbf{s}_i)_{i=0}^{\infty}$ is ultimately periodic, and its period is no more than $q^{mn} - 1$;*
- (ii) *if $c_0 \neq 0$ and $A$ is nonsingular, then $(\mathbf{s}_i)_{i=0}^{\infty}$ is periodic; conversely, if $(\mathbf{s}_i)_{i=0}^{\infty}$ is periodic whenever the initial state is of the form $(b, 0, \dots, 0)$, where $b \in \mathbb{F}_{q^m}$ with $b \neq 0$, then $c_0A$ is nonsingular.*

A TSR of order $n$ over $\mathbb{F}_{q^m}$ is *primitive* if for any choice of nonzero initial state, the sequence generated by that TSR is periodic of period $q^{mn} - 1$.

Corresponding to a *tsr-polynomial* $I_mX^n - (c_{n-1}A)X^{n-1} - \cdots - (c_1A)X - (c_0A) \in M_m(\mathbb{F}_q)[X]$, we can associate a $(m, n)$-block companion matrix $T \in M_{mn}(\mathbb{F}_q)$ of the following form

$$T = \begin{pmatrix} \mathbf{0} & \mathbf{0} & \mathbf{0} & . & . & \mathbf{0} & \mathbf{0} & c_0A \\ I_m & \mathbf{0} & \mathbf{0} & . & . & \mathbf{0} & \mathbf{0} & c_1A \\ . & . & . & . & . & . & . & . \\ . & . & . & . & . & . & . & . \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & . & . & I_m & \mathbf{0} & c_{n-2}A \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & . & . & \mathbf{0} & I_m & c_{n-1}A \end{pmatrix}, \tag{6}$$

where $c_0, c_1, \dots, c_{n-1} \in \mathbb{F}_q$, $A \in M_m(\mathbb{F}_q)$ and $\mathbf{0}$ indicates the zero matrix in $M_m(\mathbb{F}_q)$. The set of all such $(m, n)$-block companion matrices $T$ over $\mathbb{F}_q$ shall be denoted by $\mathrm{TSR}(m, n, q)$. Using a Laplace expansion or a suitable sequence of elementary column operations, we conclude that if $T \in \mathrm{TSR}(m, n, q)$ is given by (6), then $\det T = \pm \det(c_0A)$. Consequently,

$$T \in \mathrm{GL}_{mn}(\mathbb{F}_q) \Longleftrightarrow c_0 \neq 0 \text{ and } A \in \mathrm{GL}_m(\mathbb{F}_q). \tag{7}$$

where $\mathrm{GL}_m(\mathbb{F}_q)$ is the general linear group of all $m \times m$ nonsingular matrices over $\mathbb{F}_q$.

It may be noted that the block companion matrix (6) is the state transition matrix for the TSR (5). Indeed, the $k$-th state $\mathbf{S}_k := (\mathbf{s}_k, \mathbf{s}_{k+1}, \dots, \mathbf{s}_{k+n-1}) \in \mathbb{F}_{q^m}^n$ of the TSR (5) is obtained from the initial state $\mathbf{S}_0 := (\mathbf{s}_0, \mathbf{s}_1, \dots, \mathbf{s}_{n-1}) \in \mathbb{F}_{q^m}^n$ by $\mathbf{S}_k = \mathbf{S}_0 T^k$, for any $k \geq 0$.

In view of Proposition 2.2 and (7), we have that $T \in \mathrm{TSR}(m,n,q)$ is periodic if and only if $T$ has the following form

$$\begin{pmatrix} \mathbf{0} & \mathbf{0} & \mathbf{0} & . & . & \mathbf{0} & \mathbf{0} & B \\ I_m & \mathbf{0} & \mathbf{0} & . & . & \mathbf{0} & \mathbf{0} & c_1 B \\ . & . & . & . & . & . & . & . \\ . & . & . & . & . & . & . & . \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & . & . & I_m & \mathbf{0} & c_{n-2}B \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & . & . & \mathbf{0} & I_m & c_{n-1}B \end{pmatrix}, \tag{8}$$

where $c_1, \dots, c_{n-1} \in \mathbb{F}_q$ and $B \in \mathrm{GL}_m(\mathbb{F}_q)$. In what follows, we deal with periodic TSRs only, that is, a TSR of the form (8).

The following lemma reduces the calculation of an $mn \times mn$ determinant to an $m \times m$ determinant.

**Lemma 2.3.** [13] *Let $T \in \mathrm{TSR}(m,n,q)$ be given as in* (8) *and also let $F(X) \in M_m(\mathbb{F}_q[X])$ be defined by $F(X) := I_m X^n - (c_{n-1}B)X^{n-1} - \cdots - (c_1 B)X - B$. Then the characteristic polynomial of $T$ is equal to* $\det(F(X))$.

The following proposition entails that the problem of counting the number of primitive TSRs is equivalent to the enumeration of certain block companion matrices.

**Proposition 2.4.** [13] *Let $o(T)$ denote the period of the sequence generated by $T \in \mathrm{TSR}(m,n,q)$. The number of primitive TSRs of order $n$ over $\mathbb{F}_{q^m}$ is equal to the cardinality of the set*

$$\{T \in \mathrm{TSR}(m,n,q) \ : \ T \textit{ is of the form } (8) \textit{ and } o(T) = q^{mn} - 1\}.$$

The case $n = 1$ follows immediately from [10, Theorem 7.1]. In this case, the number of primitive TSRs of order one over $\mathbb{F}_{q^m}$ is given by

$$\frac{|\mathrm{GL}_m(\mathbb{F}_q)|}{(q^m - 1)} \frac{\phi(q^m - 1)}{m}.$$

The case $m = 1$ is trivial and in this case, the number of primitive TSRs of order $n$ is given by

$$\frac{\phi(q^n - 1)}{n}.$$

However, for general values of $m$ and $n$, the enumeration of primitive TSRs does not seem to be an easy problem and it still stands open. Our focus in this paper is on irreducible TSRs.

## 3. Irreducible TSRs

For a given matrix $P$, let $\psi_P(X)$ denote the characteristic polynomial of $P$. It follows from Lemma 2.3 that for any $T \in \mathrm{TSR}(m,n,q)$, the characteristic polynomial of $T$ is given by

$$\psi_T(X) = g_T(X)^m \psi_B\left(\frac{X^n}{g_T(X)}\right), \tag{9}$$

where $g_T(X) = 1 + c_1 X + \cdots + c_{n-1}X^{n-1} \in \mathbb{F}_q[X]$. It is easy to note that if $\psi_T(X)$ is irreducible, then so is $\psi_B(X)$, but the converse is not true in general.

A TSR is *primitive* (or *irreducible*) if its characteristic polynomial is primitive (or irreducible). The set of irreducible TSRs is denoted by $\mathrm{TSRI}(m,n,q)$ and the set of monic irreducible polynomials in $\mathbb{F}_q[X]$ of degree $d$ is denoted by $\mathcal{I}(d,q)$. Then the *characteristic map*

$$\Psi : M_{mn}(\mathbb{F}_q) \longrightarrow \mathbb{F}_q[X] \quad \text{defined by} \quad \Psi(T) := \det(XI_{mn} - T)$$

if restricted to the set $\mathrm{TSRI}(m,n,q)$ yields the map

$$\Psi_I : \mathrm{TSRI}(m,n,q) \longrightarrow \mathcal{I}(mn,q).$$

It was noted in [18] that the map $\Psi_I$ is not surjective in general.

The following lemma may be extracted from [10] where it is proved for primitive polynomials in some different context. However, it still holds true even for irreducible polynomials. We provide the proof of this lemma for irreducible polynomials following similar lines as in [10]. It turns out that this may be viewed as an alternative proof of a special case of [19, Theorem 2].

**Lemma 3.1.** *Let $\eta : M_m(\mathbb{F}_q) \longrightarrow \mathbb{F}_q[X]$ be defined by $\eta(A) := \det(XI_m - A)$. Then, for every $p(X) \in \mathcal{I}(m,q)$, we have,*

$$\left|\eta^{-1}\left(p(X)\right)\right| = \prod_{i=1}^{m-1}(q^m - q^i).$$

*Proof.* Let us suppose that $T \in M_m(\mathbb{F}_q)$ be such that $\eta(T) = p(X)$. Since $p(X)$ is irreducible, it is also the minimal polynomial of $T$. The invariant factors of the companion matrix $C$ of $p(X)$ and $T$ are the same and as a consequence they are similar (see [2, p. VII.32]). It follows that $\eta^{-1}(p(X)) = \{A^{-1}CA : A \in \mathrm{GL}_m(\mathbb{F}_q)\}$. Thus,

$$\left|\eta^{-1}(p(X))\right| = \frac{|\mathrm{GL}_m(\mathbb{F}_q)|}{|Z(C)|}, \quad \text{where} \quad Z(C) := \{A \in \mathrm{GL}_m(\mathbb{F}_q) : CA = AC\}.$$

Now, $C$ as a linear transformation of $\mathbb{F}_{q^m} \simeq \mathbb{F}_q^m$ is cyclic. It follows from [14, Theorem 3.16 and its corollary] that $Z(C)$ consists only of polynomials in $C$ excluding, however, the zero polynomial. Thus $Z(C) = \mathbb{F}_q[C] \setminus \{0\}$, where $\mathbb{F}_q[C]$ is the $\mathbb{F}_q$-algebra of polynomials in $C$.

The map $r(X) \mapsto r(C)$ defines a $\mathbb{F}_q$-algebra homomorphism from $\mathbb{F}_q[X]$ into $\mathbb{F}_q[C]$ with kernel the ideal of $\mathbb{F}_q[X]$ generated by $p(X)$. Hence, $\mathbb{F}_q[C]$ is isomorphic to $\mathbb{F}_q[X]/\left\langle p(X)\right\rangle$ and so its cardinality is $q^m$. Therefore, $|Z(C)| = q^m - 1$, and this completes the proof since $|\mathrm{GL}_m(\mathbb{F}_q)| = \displaystyle\prod_{i=0}^{m-1}(q^m - q^i)$. □

It follows from (9) and [18, Theorem 3] that $f(X) \in \Psi_I(\mathrm{TSRI}(m,n,q))$ if and only if $f(X)$ is irreducible and can be uniquely expressed in the form

$$g(X)^m h\left(\frac{X^n}{g(X)}\right) \tag{10}$$

for some monic irreducible polynomial $h(X) \in \mathbb{F}_q[X]$ of degree $m$ with $h(0) \neq 0$ and a not necessarily monic $g(X) \in \mathbb{F}_q[X]$ of degree at most $n-1$ with $g(0) = 1$.

**Theorem 3.2.** *The number of irreducible TSRs of order $n$ over $\mathbb{F}_{q^m}$ is given by the following*

$$|\mathrm{TSRI}(m,n,q)| = |\Psi_I(\mathrm{TSRI}(m,n,q))| \prod_{i=1}^{m-1} (q^m - q^i).$$

*Proof.* Let us assume that $f(X) \in \Psi_I(\mathrm{TSRI}(m,n,q))$; then $f(X)$ can be uniquely expressed in the form (10). Moreover, there is $T \in \mathrm{TSRI}(m,n,q)$ such that $\psi_T(X) = f(X)$. Clearly $g_T(X) = g(X)$ and $\psi_B(X) = h(X)$. The number of such $T$ is equal to the number of possible values of $B$ with $\psi_B(X) = h(X)$. Since $h(X)$ is irreducible, by Lemma 3.1, the number of such $B$ is $\prod_{i=1}^{m-1}(q^m - q^i)$. □

The case $m = 1$ is trivial and in this case, the number of irreducible TSRs of order $n$ is given by,

$$\frac{1}{n}\sum_{d|n} \mu(d)\, q^{\frac{n}{d}}. \tag{11}$$

In the case $n = 1$, the number of irreducible TSRs of order one is given by

$$\frac{1}{m}\prod_{i=1}^{m-1}(q^m - q^i)\sum_{d|m}\mu(d)\, q^{\frac{m}{d}}. \tag{12}$$

In view of Theorem 3.2, it is sufficient to enumerate the polynomials in the set $\Psi_I(\mathrm{TSRI}(m,n,q))$ to find the number of irreducible TSRs. In fact, Ram [18] enumerates TSRs of order two. Moreover, he re-derives a theorem of Carlitz [3] about the number of self reciprocal irreducible monic polynomials of a given degree over a finite field. In this section, we give a short proof of [18, Theorem 8] using a generalization due to Ahmadi [1] of a result of Carlitz.

**Proposition 3.3.** [1] *Let $e(X) = a_1X^2 + b_1X + c_1$ and $g(x) = a_2X^2 + b_2X + c_2$ be two relatively prime polynomials in $\mathbb{F}_q[X]$ with $\max(\deg(e), \deg(g)) = 2$. Also let $\mathcal{I}(e,g,m,q)$ be the set of monic irreducible polynomials $h(X)$ of degree $m > 1$ over $\mathbb{F}_q$ such that*

$$g(X)^m h\left(\frac{e(X)}{g(X)}\right)$$

*is irreducible over $\mathbb{F}_q$. Then*

$$|\mathcal{I}(e,g,m,q)| = \begin{cases} 0 & \text{if } b_1 = b_2 = 0 \text{ and } q \text{ is even;} \\ \dfrac{1}{2m}(q^m - 1) & \text{if } q \text{ is odd and } m = 2^\ell,\ \ell \geq 1; \\ \dfrac{1}{2m}\displaystyle\sum_{d|m, d \text{ odd}} \mu(d) q^{\frac{m}{d}} & \text{otherwise.} \end{cases}$$

We use the above proposition to give a short proof of [18, Theorem 8] to count the number of irreducible TSRs of order two over $\mathbb{F}_{q^m}$.

**Theorem 3.4.** *For $m > 1$, we have,*

$$|\Psi_I(\mathrm{TSRI}(m,2,q))| = \begin{cases} \dfrac{q}{2m}(q^m-1) & \text{if } q \text{ is odd and } m = 2^\ell; \\ \dfrac{q}{2m}\displaystyle\sum_{d|m, d \text{ odd}} \mu(d) q^{\frac{m}{d}} & \text{if } q \text{ is odd and } m = 2^\ell k, \\ & \text{and } k \geq 3 \text{ is odd}; \\ \dfrac{q-1}{2m}\displaystyle\sum_{d|m, d \text{ odd}} \mu(d) q^{\frac{m}{d}} & \text{otherwise.} \end{cases}$$

*Proof.* For every $a \in \mathbb{F}_q$, let $\mathcal{I}_m(a)$ denote the set of monic irreducible polynomials $h(X)$ of degree $m > 1$ over $\mathbb{F}_q$ such that

$$(aX+1)^m h\left(\frac{X^2}{aX+1}\right)$$

is irreducible over $\mathbb{F}_q$. A direct application of Proposition 3.3 for $e(X) = X^2$ and $g(X) = aX + 1$ yields

$$|\mathcal{I}_m(a)| = \begin{cases} 0 & \text{if } a = 0 \text{ and } q \text{ is even;} \\ \dfrac{1}{2m}(q^m-1) & \text{if } q \text{ is odd and } m = 2^\ell,\ \ell \geq 1; \\ \dfrac{1}{2m}\displaystyle\sum_{d|m, d \text{ odd}} \mu(d) q^{\frac{m}{d}} & \text{otherwise.} \end{cases}$$

In view of (10), the proof is complete after the following observation

$$|\Psi_I(\mathrm{TSRI}(m,2,q))| = \sum_{a \in \mathbb{F}_q} |\mathcal{I}_m(a)| = \begin{cases} |\mathcal{I}_m(1)|q & \text{if } q \text{ is odd;} \\ |\mathcal{I}_m(1)|(q-1) & \text{if } q \text{ is even.} \end{cases}$$

□

Combining Theorem 3.2 and Theorem 3.4, we give an alternative proof of Theorem 8 in [18].

**Theorem 3.5.** *For $m > 1$, the number of irreducible TSRs of order two over $\mathbb{F}_{q^m}$ is given by*

$$|\mathrm{TSRI}(m,2,q)| = \begin{cases} \dfrac{q}{2m}\displaystyle\prod_{i=0}^{m-1}(q^m - q^i) & \text{if } q \text{ is odd and } m = 2^\ell; \\ \dfrac{q}{2m}\displaystyle\prod_{i=1}^{m-1}(q^m - q^i)\sum_{d|m, d \text{ odd}} \mu(d) q^{\frac{m}{d}} & \text{if } q \text{ is odd, } m = 2^\ell k, \\ & \text{and } k \geq 3 \text{ is odd}; \\ \dfrac{q-1}{2m}\displaystyle\prod_{i=1}^{m-1}(q^m - q^i)\sum_{d|m, d \text{ odd}} \mu(d) q^{\frac{m}{d}} & \text{otherwise.} \end{cases}$$

## 4. Asymptotic analysis of the number of irreducible TSRs of order two

Although we already know the explicit formula for the number of irreducible TSRs of order two. However, in this section we will be doing the asymptotic analysis for the number of irreducible TSRs of order two by using some results due to Cohen [5]. For the convenience of the reader, we recall here some notation and a theorem of Cohen about the distribution of polynomials over finite fields [5].

Let $e, g \in \mathbb{F}_q[X]$ be monic relatively prime polynomials satisfying the following conditions:

(1) $n = \deg e > \deg g \geq 0$;

(2) $\dfrac{e(X)}{g(X)} \neq \dfrac{e_1(X^p)}{g_1(X^p)}$ for any $e_1, g_1 \in \mathbb{F}_q[X]$.

Further, let $\mathrm{G}^{e,g}$ be the Galois group of $e(X) - tg(X)$ over $\mathbb{F}_{q^m}(t)$, where $t$ is an indeterminate, with splitting field $K$. We regard $\mathrm{G}^{e,g}$ as a subgroup of $\mathcal{S}_n$, the $n$th symmetric group. Let $\mathrm{G}^{e,g}_\lambda$ be the set of elements of $\mathrm{G}^{e,g}$ having the same cycle pattern $\lambda$. For any $\sigma \in \mathrm{G}^{e,g}$, let $K_\sigma$ denote the subfield of $K$ fixed under $\sigma$.

Moreover, let $\mathbb{F}^{'}_{q^m} (= \mathbb{F}_{(q^m)^s}$ for some $s \geq 1)$ be the largest algebraic extension of $\mathbb{F}_{q^m}$ in $K$. Let $\widehat{\mathrm{G}}^{e,g} = \{\sigma \in \mathrm{G}^{e,g} \ : \ K_\sigma \cap \mathbb{F}^{'}_{q^m} = \mathbb{F}_{q^m}\}$ and put $\widehat{\mathrm{G}}^{e,g}_\lambda = \widehat{\mathrm{G}}^{e,g} \cap \mathrm{G}^{e,g}_\lambda$ for any cycle pattern $\lambda$. We note that $\sigma \in \widehat{\mathrm{G}}^{e,g}$ if and only if $K_\sigma \cap \mathbb{F}^{'}_{q^m}(t) = \mathbb{F}_{q^m}(t)$.

With these notations, we recall a lemma that is used in the sequel [5, Lemma 1].

**Lemma 4.1.** [5] *With the notation as above, we have*

$$\left|\widehat{\mathrm{G}}^{e,g}\right| = \frac{\phi(s)}{s} \left|\mathrm{G}^{e,g}\right|,$$

*where $\phi$ is Euler's totient function.*

It is also mentioned in [5] that if $\widehat{\mathrm{G}}^{e,g}$ is isomorphic to the symmetric group $\mathcal{S}_n$ and $\lambda$ is a cycle of order $n$, then

$$\frac{\left|\widehat{\mathrm{G}}^{e,g}_\lambda\right|}{\left|\widehat{\mathrm{G}}^{e,g}\right|} = \frac{1}{n}. \tag{13}$$

Throughout this section, all the constants implied by $O$-terms depend only on $n = \deg\left(e(X) - tg(X)\right)$.

**Proposition 4.2.** [5] *Let $e, g \in \mathbb{F}_q[X]$ be as stated above. Also let $\mathcal{I}(e, g, m, q)$ be the set of monic irreducible polynomials $h(X)$ of degree $m$ over $\mathbb{F}_q$ such that*

$$g(X)^m h\left(\frac{e(X)}{g(X)}\right)$$

*is irreducible over $\mathbb{F}_q$. Then*

$$|\mathcal{I}(e, g, m, q)| = \frac{|\widehat{\mathrm{G}}^{e,g}_n|}{|\widehat{\mathrm{G}}^{e,g}|} \frac{q^m}{m} + O\left(q^{\frac{m}{2}}\right).$$

*Moreover, when $\widehat{\mathrm{G}}^{e,g} = \mathcal{S}_n$,*

$$|\mathcal{I}(e, g, m, q)| = \frac{1}{mn} q^m + O\left(q^{\frac{m}{2}}\right).$$

For $e(X) = X^n$ and $g(X) = 1 + a_1X + \cdots + a_{n-1}X^{n-1}$, we shall alternatively denote the Galois group $\mathrm{G}^{e,g}$ of $X^n - tg(x) \in \mathbb{F}_{q^m}(t)[X]$ by $\mathrm{G}^{\bar{a}}$, where $\bar{a} = (a_1, \ldots, a_{n-1}) \in \mathbb{F}_q^{n-1}$. Using this notation, we give a formula for the cardinality of the set $\Psi_I\left(\mathrm{TSRI}(m, n, q)\right)$ and we further prove that this is indeed an asymptotic formula in some special cases.

**Theorem 4.3.** *Let $m > 1$ and $g(X) = 1 + a_1X + \cdots + a_{n-1}X^{n-1}$. Assume $\mathrm{G}^{\bar{a}}$ is the Galois group of $X^n - tg(X)$ over $\mathbb{F}_{q^m}(t)$, where $\bar{a} = (a_1, \ldots, a_{n-1})$. Then for $n > 1$, we have*

$$|\Psi_I\left(\mathrm{TSRI}(m, n, q)\right)| = c\frac{q^m}{m} + O\left(q^{n-1+\frac{m}{2}}\right),$$

*where $c = \sum_{\bar{a}\in\mathbb{F}_q^{n-1}} \frac{|\widehat{\mathrm{G}}_n^{\bar{a}}|}{|\widehat{\mathrm{G}}^{\bar{a}}|}$ and for $n = 1$, we have*

$$|\Psi_I\left(\mathrm{TSRI}(m, n, q)\right)| = \frac{1}{m}q^m + O\left(q^{\frac{m}{2}}\right).$$

*Proof.* Assume that $n > 1$ and for every $\bar{a} = (a_1, \ldots, a_{n-1}) \in \mathbb{F}_q^{n-1}$, let $\mathcal{I}_m(\bar{a})$ denote the set of monic irreducible polynomials $h(X)$ of degree $m > 1$ over $\mathbb{F}_q$ such that

$$g(X)^m h\left(\frac{X^n}{g(X)}\right)$$

is irreducible over $\mathbb{F}_q$, where $g(X) = 1+a_1X+\cdots+a_{n-1}X^{n-1}$. A direct application of Proposition 4.2 with $e(X) = X^n$ and $g(X) = 1 + a_1X + \cdots + a_{n-1}X^{n-1}$ yields

$$|\mathcal{I}_m(\bar{a})| = \frac{|\widehat{\mathrm{G}}_n^{\bar{a}}|}{|\widehat{\mathrm{G}}^{\bar{a}}|}\frac{q^m}{m} + O\left(q^{\frac{m}{2}}\right).$$

However, in the particular case when $\widehat{\mathrm{G}}^{\bar{a}} = \mathcal{S}_n$, we have

$$|\mathcal{I}_m(\bar{a})| = \frac{1}{mn}q^m + O\left(q^{\frac{m}{2}}\right).$$

In view of (10), we have

$$|\Psi_I\left(\mathrm{TSRI}(m, n, q)\right)| = \sum_{\bar{a}\in\mathbb{F}_q^{n-1}} |\mathcal{I}_m(\bar{a})| = c\frac{q^m}{m} + O\left(q^{n-1+\frac{m}{2}}\right),$$

where $c = \sum_{\bar{a}\in\mathbb{F}_q^{n-1}} \frac{|\widehat{\mathrm{G}}_n^{\bar{a}}|}{|\widehat{\mathrm{G}}^{\bar{a}}|}$.

For $n = 1$, we have $e(X) = X$ and $g(X) = 1$. Thus, $\widehat{\mathrm{G}}_1^{e,g} = \widehat{\mathrm{G}}^{e,g} = \mathrm{G}^{e,g} = \mathcal{S}_1$ and in this case, the proof follows from Proposition 4.2. □

We remark that in the proof of the above theorem, $g(X)$ is not necessarily a monic polynomial, but we could still apply Proposition 4.2.

The following theorem is an easy consequence of Theorem 4.3 and gives a formula for the number of irreducible TSRs.

**Theorem 4.4.** *Let us suppose that $m > 1$. Then the number $|\mathrm{TSRI}(m, n, q)|$ of irreducible TSRs of order $n > 1$ over $\mathbb{F}_{q^m}$ satisfies*

$$|\mathrm{TSRI}(m, n, q)| = c\frac{q^m}{m}\prod_{i=1}^{m-1}(q^m - q^i) + O\left(q^{m^2+n-1-\frac{m}{2}}\right),$$

*where* $c = \sum_{\bar{a}\in\mathbb{F}_q^{n-1}} \frac{|\widehat{\mathrm{G}}_n^{\bar{a}}|}{|\widehat{\mathrm{G}}^{\bar{a}}|}$. *For* $n = 1$, *we have*

$$|\mathrm{TSRI}(m,n,q)| = \frac{1}{m} q^m \prod_{i=1}^{m-1} (q^m - q^i) + O\left(q^{m^2 - \frac{m}{2}}\right).$$

*Proof.* The proof follows immediately from Theorem 3.2 and Theorem 4.3. □

**Remark 4.5.** The explicit computation of the constant $c$ in Theorem 4.3 seems a rather difficult problem. Without knowing the behaviour of $c$, it is not clear if the $c\frac{q^m}{m}$ term can be absorbed into the big Oh term; if this happens, we no longer have an asymptotic formula. When $m < 2(n-1)$, it is not clear if $cq^m$ is asymptotically bigger than $q^{n-1+m/2}$. Thus, unless we know the asymptotics of $c$ as a power of $q$ for large values of $q$, Theorem 4.3 does not give an asymptotic formula for $|\Psi_I(\mathrm{TSRI}(m,n,q))|$. The same holds true for Theorem 4.4.

It is clear that for $n = 1$, the first term ($d = 1$) in (12) is exactly the same as the main term in the formula of Theorem 4.4. For the case $n = 2$, we explicitly compute the value of $c$ in the following theorem allowing us to compare the main term in the formula of Theorem 4.4 with the first term in the formula of Theorem 3.5. When $n = 2$, we prove that the main terms $c\frac{q^m}{m}$ and $c\frac{q^m}{m}\prod_{i=1}^{m-1}(q^m - q^i)$ of Theorem 4.3 and Theorem 4.4, respectively, do not get absorbed in the big Oh term.

**Theorem 4.6.** *Let* $p$ *be the characteristic of the field* $\mathbb{F}_{q^m}$. *For* $n = 2$, *the value of the constant* $c$ *in Theorem 4.4 is* $\frac{q}{2}$ *whenever* $p \neq 2$, *and* $\frac{q-1}{2}$ *if* $p = 2$.

*Proof.* For $n = 2$, we have $e(X) = X^2$, $g(X) = aX + 1$, and $\bar{a} = a \in \mathbb{F}_q$. We consider two different cases depending upon the characteristic $p$ of the field $\mathbb{F}_{q^m}$.

**Case 1:** Suppose $p \neq 2$. Then for each $\bar{a} = a$ in $\mathbb{F}_q$, $X^2 - t(aX+1)$ is irreducible and separable over $\mathbb{F}_{q^m}(t)$ and thus $\mathrm{G}^{\bar{a}} = \mathcal{S}_2$.

Let $K$ be splitting field of $X^2 - t(aX+1)$ over $\mathbb{F}_{q^m}(t)$ and let $\mathbb{F}'_{q^m}(= \mathbb{F}_{(q^m)^s}$ for some $s \geq 1$) be the largest algebraic extension of $\mathbb{F}_{q^m}$ in $K$. We have $\mathbb{F}_{q^m}(t) \subseteq \mathbb{F}'_{q^m}(t) \subseteq K$. Since $[K : \mathbb{F}_{q^m}(t)] = 2$, $\mathbb{F}'_{q^m}(t)$ is either equal to $K$ or $\mathbb{F}_{q^m}(t)$. But the irreducibility of the polynomial $X^2 - t(aX+1)$ over $\mathbb{F}'_{q^m}(t)$ ensures that $\mathbb{F}'_{q^m}(t) \neq K$. Therefore $\mathbb{F}'_{q^m}(t) = \mathbb{F}_{q^m}(t)$ and hence, $s = 1$. Thus using Lemma 4.1, we have $\widehat{\mathrm{G}}^{\bar{a}} = \mathrm{G}^{\bar{a}} = \mathcal{S}_2$. Now by using (13), we obtain

$$c = \sum_{\bar{a}=a\in\mathbb{F}_q} \frac{|\widehat{\mathrm{G}}_2^{\bar{a}}|}{|\widehat{\mathrm{G}}^{\bar{a}}|} = \frac{q}{2}.$$

**Case 2:** Suppose $p = 2$. Then for each $\bar{a} = a \neq 0$ in $\mathbb{F}_q$, $X^2 - t(aX+1)$ is irreducible and separable over $\mathbb{F}_{q^m}(t)$ and thus $\mathrm{G}^{\bar{a}} = \mathcal{S}_2$. Following similar arguments as before, we deduce that for $\bar{a} = a \neq 0$, $\widehat{\mathrm{G}}^{\bar{a}} = \mathrm{G}^{\bar{a}} = \mathcal{S}_2$.

However, when $\bar{a} = a = 0$, the polynomial $x^2 - t$ is irreducible, but not separable over $\mathbb{F}_{q^m}(t)$. Thus, $\widehat{\mathrm{G}}^0 = \mathrm{G}^0 = \mathcal{A}_2$ and hence $\left|\widehat{\mathrm{G}}_2^0\right| = 0$. Again Equation (13) yields

$$c = \sum_{\bar{a}=a\in\mathbb{F}_q} \frac{|\widehat{\mathrm{G}}_2^{\bar{a}}|}{|\widehat{\mathrm{G}}^{\bar{a}}|} = \sum_{\bar{a}=a\neq 0\in\mathbb{F}_q} \frac{|\widehat{\mathrm{G}}_2^{\bar{a}}|}{|\widehat{\mathrm{G}}^{\bar{a}}|} = \frac{q-1}{2}.$$

□

## 5. An asymptotic formula for the number of irreducible TSRs of any order when $q$ is odd

In this section, we prove an asymptotic formula for the number of irreducible TSRs of any order when $q$ is odd by using some previous results due to Cohen [7].

It may be noted that $f$ is necessarily monic of degree $mn$ in (10) and $f(0) = h(0) \neq 0$. Its (monic) reciprocal is $f^*(X) = X^{\deg f} f(1/X)/f(0)$. Of course, $f$ is irreducible if and only if $f^*$ is irreducible. From (10)

$$f^*(X) = X^{mn} g(1/X)^m h\left(\frac{1}{X^n g(1/X)}\right)/f(0) = h^*(\bar{g}^*(X)), \tag{14}$$

since $f(0) = h(0) \neq 0$ and $\bar{g}(X) = Xg(X)$. Thus, from now on, if we replace $g$ by the reciprocal $X^n + a_1X^{n-1} + \cdots + a_{n-1}X$ of $\bar{g}$, we have that $M(m,n,q) := |\Psi_I(\mathrm{TSRI}(m,n,q))|$ is the number of irreducible polynomials in $\mathbb{F}_q[X]$ of the form $h(g(X))$, where $h$ is a monic polynomial of degree $m$ (necessarily irreducible) and $g$ is a monic polynomial of degree $n$ (with $g(0) = 0$), as described. Suppose $\alpha$ is a root in $\mathbb{F}_{q^m}$ of a monic irreducible polynomial $h(X) \in \mathbb{F}_q[X]$ of degree $m$. Then $h(g(X))$ is irreducible in $\mathbb{F}_q[X]$ if and only if $g(X) - \alpha$ is irreducible in $\mathbb{F}_{q^m}[X]$. Hence $mM(m,n,q)$ is sum over all $(n-1)$-tuples $\bar{a}$ of the number of $\alpha \in \mathbb{F}_{q^m}$, not in a proper subfield, such that $g(X) - \alpha$ is irreducible in $\mathbb{F}_{q^m}$.

When $m = 1$, then $M(1,n,q)$ is simply the number of irreducible polynomials of degree $n$ over $\mathbb{F}_q$, given by the well-known formula. So suppose $m > 1$ and define $N(m,n,q)$ to be the sum over $\bar{a}$ of the total number of $\alpha \in \mathbb{F}_{q^m}$ such that $g(X) - \alpha$ is irreducible in $\mathbb{F}_{q^m}$. Then

$$N(m,n,q) = mM(m,n,q) + O(q^{n-1+m/2}). \tag{15}$$

Let $K_q$ be the algebraic closure of the field $\mathbb{F}_q$ (and so of $\mathbb{F}_{q^m}$). Let $F(X) = g(X) - t$, where $t$ is an indeterminate. For given $\bar{a}$, $\mathrm{G}^{\bar{a}}$ denotes the Galois group of $g(X) - t$ over $\mathbb{F}_{q^m}(t)$, where $t$ is an indeterminate. It has as a normal subgroup $\widehat{\mathrm{G}}^{\bar{a}}$, the Galois group of $g(X) - t$ over $K_q(t)$. An important criterion for $\widehat{\mathrm{G}}^{\bar{a}}$ to be the full symmetric group $\mathcal{S}_n$ derives from Theorem 4.8 of [7].

**Lemma 5.1.** *Let $g(X) \in \mathbb{F}_q[X]$ be monic of degree $n$ and indecomposable over $\mathbb{F}_q$ (i.e, $g$ is not a composition $g = g_1(g_2)$ of polynomials $g_1(X), g_2(X) \in \mathbb{F}_q[X]$, where* $\deg(g_i) \geq 2,\ i = 1, 2$*). Suppose that, for some $\theta \in K_q$, $g(X) - \theta$ factorizes over $K_q$ as $(X - \beta)^2 E(X)$ for some square-free polynomial $E$ (with $E(\beta) \neq 0$). Then the Galois group of $g(X) - t$ over $K_q(t)$ is $\mathcal{S}_n$.*

We can suppose $n \geq 3$. It turns out we have to exclude from consideration $(n-1)$-tuples $\bar{a}$ of a certain form as we now describe. Let $p$ be the characteristic of $\mathbb{F}_q$, i.e., $q$ is a power of the prime $p$. The polynomial $g(X) = X^n + a_1X^{n-1} + \cdots + a_{n-1}X$ is said to be of form (16) if we can express it in the form

$$XA(X^p) + B(X^p), \tag{16}$$

where $A, B$ are polynomials, i.e., $n \equiv 0, 1 \pmod{p}$ and $a_i = 0$, whenever $i \not\equiv 0, 1 \pmod{p}$. Given $a_1, \ldots, a_{n-2} \in \mathbb{F}_q$, set $F_0(X) = g(X) - a_{n-1}X = X^n + \sum_{i=1}^{n-2} a_i X^{n-i}$. Observe that $F_0$ has form (16) if and only if $g$ has form (16) for any $a_{n-1} \in \mathbb{F}_q$.

We remark further that if $p = 2$, then every polynomial $g$ has the form (16). Hence, it is necessary from now to impose the restriction that $q$ is odd.

**Lemma 5.2.** *Suppose $q$ is odd and $n \geq 3$. Let $a_1, \ldots, a_{n-2}$ be any elements of $\mathbb{F}_q$ such that $F_0$ does not have the form* (16). *Then, for all but $O(1)$ choices of non-zero elements $a_{n-1} \in \mathbb{F}_q$, $\widehat{\mathrm{G}}^{\bar{a}} = \mathcal{S}_n$. (Here, as throughout, the implied constant depends only on $n$.)*

*Proof.* It has to be shown that, for all but $O(1)$ choices of $a_{n-1}$, $g$ is indecomposable over $\mathbb{F}_{q^m}$ and, for any $\theta \in K_q$, either $g(X) - \theta$ is square-free or factorizes as $(X - \beta)^2 E(X)$, as described in Lemma 5.1. The proof of this follows exactly that of Lemma 5 of [6], in the special case in which $s = 2$ and the polynomials $F_0, F_1, F_2$ (in the notation of Theorem 3 of [6]) are, respectively, $F_0$ as defined here, $F_1(X) = X, F_2(X) = 1$. The proof of [6], Lemma 5, is derived from that of Lemmas 6, 7, and the identical arguments can be used in this particular situation. (Note, in particular, that assumption $p \nmid n$ of [6], Theorem 3, is not required at this stage.) The main thrust of the proof of [6], Lemma 6, is that with $O(1)$ exceptional values of $a_{n-1}$, $g$ is indecomposable (actually even over $K_q$). Otherwise, $F_0, F_1, F_2$ would be "totally composite", which is evidently not the case. Further, the assumption that $F_0, F_1, F_2$ are linearly independent over $\mathbb{F}_{q^m}(X^p)$ of [6], Theorem 3, in our situation, is a consequence of the assumption that $F_0$ does not have form (16).

The conclusion of [6], Lemma 7, is that if $a_{n-1}$ is one of the $q - O(1)$ (non-zero) elements of $\mathbb{F}_q$ that have not been excluded, then, for every $\theta \in K_q$, either $g(X) - \theta$ is square-free or has the form $(X - \beta)^2 E(X)$. Now, let $\beta \in K_q$ be any root of the formal derivative $g'(X)$. Indeed, since $g$ does not have the form (16), there is such an element $\beta$. Set $\theta = g(\beta)$. Then $\beta$ is a repeated root of $g(X) - \theta$ of multiplicity 2 and there are no other repeated roots of $g(X) - \theta$. Then Lemma 5.1 applies and we conclude that $\widehat{\mathrm{G}}^{\bar{a}} = \mathcal{S}_n$. □

**Theorem 5.3.** *Suppose $q$ is odd, $n \geq 3$ and $m \geq 2$. Then*

$$N(m, n, q) = \frac{q^{m+n-1}}{n} + O(q^{m+n-2}).$$

*Proof.* There are in total $q^{n-1}$ choices of $\bar{a}$ in the polynomial $g$. We show that for all but $O(q^{n-2})$ of them $\widehat{\mathrm{G}}^{\bar{a}} = \mathcal{S}_n$, whence, by [5, Theorem 1] for every non-excluded choice $\bar{a}$, the number of $\alpha \in \mathbb{F}_{q^m}$ such that $g(X) - \alpha$ is irreducible is

$$\frac{q^m}{n} + O(q^{m/2}). \tag{17}$$

Given $a_1, \ldots, a_{n-2}$ in $\mathbb{F}_q$, let the implied constant in the number of values of $a_{n-1}$ to be excluded be bounded above by $d(= d_n)$. Altogether, this excludes at most $dq^{n-2}$ choices of $\bar{a}$. When $n \not\equiv 0, 1 \pmod{p}$, by Lemma 5.2, for the remaining choices of $\bar{a}$, $\widehat{\mathrm{G}}^{\bar{a}} = \mathcal{S}_n$ and, by (17),

$$N(m, n, q) \geq \frac{q^{m+n-1} - dq^{m+n-2}}{n} + O(q^{n-1+m/2}) = \frac{q^{m+n-1}}{n} + O(q^{m+n-2}). \tag{18}$$

When $n \equiv 0, 1 \pmod{p}$, further values of $\bar{a}$ have to be excluded because, in Lemma 5.2, $g$ has the form (16). In particular, when $p|n$, then these further excluded values all have $a_1 = 0$, whence their total number does not exceed $q^{n-2}$. Similarly, if $n \geq 3$ and $n \equiv 1 \pmod{p}$, then $n \geq p + 1 \geq 4$ and all further excluded $\bar{a}$ have $a_2 = 0$. Thus their total number again does not exceed $q^{n-2}$. The argument in these cases then proceeds as at (18) with $d$ replaced by $d + 1$. □

**Corollary 5.4.** *Suppose $q$ is odd, $n \geq 3$ and $m \geq 2$. Then*

$$M(m,n,q) = |\Psi_I(\mathrm{TSRI}(m,n,q))| = \frac{q^{m+n-1}}{mn} + O(q^{m+n-2}/m).$$

*Proof.* This follows from Theorem 5.3, along with (15) and the definition of $M$. □

From Corollary 5.4, when $q$ is odd, for $q > q_n$ the constant $c$ in Theorem 4.3 is positive.

**Theorem 5.5.** *Suppose that $q$ is odd and $m > 1$. Then the number $|\mathrm{TSRI}(m,n,q)|$ of irreducible TSRs of order $n > 2$ over $\mathbb{F}_{q^m}$ satisfies*

$$|\mathrm{TSRI}(m,n,q)| = \frac{q^{m+n-1}}{mn}\prod_{i=1}^{m-1}(q^m - q^i) + O\left(q^{m^2+n-2}/m\right).$$

*Proof.* The proof follows immediately from Theorem 3.2 and Corollary 5.4. □

We note that the main term in Theorem 5.3 corresponds to the main term in Theorem 4.3, however, the error term is slightly increased in most of the cases. It may be interesting to determine if the formula in Theorem 4.3 and hence in Theorem 4.4 is asymptotic in nature when $q$ is even.

## Acknowledgments

Sartaj Ul Hasan and Qiang Wang would like to thank Daqing Wan for some helpful discussions.

## References

[1] O. Ahmadi, *Generalization of a theorem of Carlitz*, Finite Fields Appl. 17, 473–480, 2011.

[2] N. Bourbaki, *Algèbre*, Chapitres 4 à 7, Masson, Paris, 1981.

[3] L. Carlitz, *Some theorems on irreducible reciprocal polynomials over a finite field*, J. Reine Angew. Math. 227, 212-220, 1967.

[4] E. Chen and D. Tseng, *The splitting subspace conjecture*, Finite Fields Appl. 24, 15–28, 2013.

[5] S. D. Cohen, *The distribution of polynomials over finite fields*, Acta Arith. 17, 255–271, 1970.

[6] S. D. Cohen, *Uniform distribution of polynomials over finite fields*, J. London Math. Soc. (2) 6 (1972), 93-102.

[7] S. D. Cohen, *Some function field estimates with applications*, Number theory and its applications (Ankara, 1996), 23-45, Lecture Notes in Pure and Appl. Math., 204, Dekker, New York, 1999.

[8] M. Dewar and D. Panario, *Linear transformation shift registers*, IEEE Trans. Inform. Theory 49, 2047–2052, 2003.

[9] M. Dewar and D. Panario, *Mutual irreducibility of certain polynomials*, in Finite Fields and Applications, Vol. 2948 of Lecture Notes in Comput. Sci., 59–68, Springer, Berlin, 2004.

[10] S. R. Ghorpade, S. U. Hasan and M. Kumari, *Primitive polynomials, Singer cycles, and word oriented linear feedback shift registers*, Des. Codes Cryptogr. 58, 123–134, 2011.

[11] S. R. Ghorpade and S. Ram, *Block companion Singer cycles, primitive recursive vector sequences, and coprime polynomial pairs over finite fields*, Finite Fields Appl. 17, 461–472, 2011.

[12] S. W. Golomb and G. Gong, *Signal Design for Good Correlation*, Cambridge University Press, 2005.

[13] S. U. Hasan, D. Panario and Q. Wang, *Word-oriented transformation shift registers and their linear complexity*, in Proceedings of SEquences and Their Applications - SETA 2012, Vol. 7280 of Lecture Notes in Comput. Sci., 190–202, Springer, Berlin, 2012.

[14] N. Jacobson, *Basic Algebra I*, 2nd Ed., W. H. Freeman, New York, 1985.

[15] R. Lidl and H. Niederreiter, *Finite Fields*, 2nd Ed., Cambridge University Press, Cambridge, 1997.

[16] H. Niederreiter, *The multiple-recursive matrix method for pseudorandom number generation*, Finite Fields Appl. 1, 3–30, 1995.

[17] B. Preneel, *Introduction to the Proceedings of the Second Workshop on Fast Software Encryption*, Vol. 1008 of Lecture Notes in Comput. Sci., 1–5, Springer, Berlin, 1995.

[18] S. Ram, *Enumeration of linear transformation shift registers*, to appear in Des. Codes Cryptogr., 2014.

[19] I. Reiner, *On the number of matrices with given characteristic polynomial*, Illinois J. Math. 5, 324-329, 1961.

[20] B. Tsaban and U. Vishne, *Efficient feedback shift registers with maximal period*, Finite Fields Appl. 8, 256–267, 2002.

[21] G. Zeng, W. Han and K. He, *Word-oriented feedback shift register: $\sigma$-LFSR*, http://eprint.iacr.org/2007/114 (Cryptology ePrint Archive: Report 2007/114).

School of Mathematics and Statistics, University of Glasgow
Glasgow G12 8QW, Scotland
*E-mail address*: `Stephen.Cohen@glasgow.ac.uk`

Scientific Analysis Group, Defence Research and Development Organisation
Metcalfe House, Delhi 110054, India
*E-mail address*: `sartajulhasan@gmail.com`

School of Mathematics and Statistics, Carleton University, Ottawa, K1S 5B6, Canada
*E-mail address*: `daniel@math.carleton.ca`

School of Mathematics and Statistics, Carleton University, Ottawa, K1S 5B6, Canada
*E-mail address*: `wang@math.carleton.ca`